SIEM Essentials SOW Draft

When writing a SoW always use the template at https://splunk.box.com/s/6rityszely8hroou34c6smn3xhfzfg1j

Splunk App for Enterprise Security – **SIEM Essentials Offering** – Standard Deployment

Only edit estimated times – **DO NOT edit tasks** – Use the Custom SOW for that

Statement of Work

Services
Splunk Professional Services ("PS") will provide the following Services for Customer:

#	Task	Notes	Estimated Days	(INTERNAL) Consultant Skill
Part 1: Kickoff		Consultants: Onboarding Specialist, Enterprise Security Specialist		(Remote)
1.1	Conduct a kick-off call at least two (2) weeks prior to the start of this project.	The kick-off call will cover the following topics: • SOW • Architecture review • Data source review • Data source access • Server access • Personnel logistics	-	SKILLI-PS-General
Part 2: Architecture Planning		Consultant: Enterprise Security Specialist		(Remote)
2.1	Plan Splunk Architecture.	Architecture Planning includes: • Defining data collection strategy • Review and document proposed system architecture • Review syslog setup and collection method/filters/ports • Review and validate network and access control requirements ◦ Including firewall change request processes • Discuss Assets and Identities to prepare for collection and onboarding into Enterprise Security • Anticipated artifact: Finalized Splunk Architecture **Reference Hardware** • Search Head (Ad-hoc) Reference Hardware[1] • Search Head (Enterprise Security)[2] • Indexer (Enterprise Security)[3]		SKILLI-PS-SecurityEnabled
Part 3: Splunk Installation		Consultant: Onboarding Specialist		(Remote)
3.1	Configure Syslog Architecture.	This configuration task includes: • Configuration of syslog aggregator (rsyslog/syslog-ng) ◦ Note if syslog-ng is utilized customer is responsible for installation PS can assist only with tcp input and event routing • Configuration of syslog inputs/ • Configure up to four (4) dedicated universal forwarders for syslog forwarding		SKILLI-PS-General

3.2	Configure Splunk Enterprise.	This configuration task includes:
		• Splunk server configuration
		  ◦ Two (2) deployment servers
		  ◦ Two (2) search heads
		  ◦ One (1) master/ utility server [DMC/ITSI]
		  ◦ Three (3) indexers
		• Splunk Forwarder Deployment
		  ◦ Ensure change control process is documented
		  ◦ Review deployment strategy
		  ◦ Prepare Universal Forwarder packages (Windows & Linux)
		  ◦ Configure Server Classes
				SKILLI-PS-General

Part 4: Data On-Boarding, Enterprise Security, Dashboards, Initial Use Cases		Consultant: Onboarding Specialist		(Remote)

4.1	Data Acquisition, Extraction & Enrichment	This task includes: • Technology Add-On (TA) installation for data sources • Configuration for collection of data sources • Including access control/index configuration • Onboard and configure nine (9) essential data sources. • Mail • DNS • Authentication • Endpoint Antimalware • Web Proxy Request • User Activity • Audit Trail • Network Communication • Network Intrusion Detection • Test/Validate TAs		SKILLI-PS-General
4.2	Validate Data in Splunk	Ensure data in Splunk matches the appropriate Common Information Model[4] standards for data normalisation. This validates Technology Add-Ons (TAs) are functioning correctly.		SKILLI-PS-General (Remote)
4.3	Enterprise Security Installation	This task includes: • Installation and tuning of Splunk App for Enterprise Security (ES)		SKILLI-PS-General (Remote)
4.4	Enterprise Security Dashboards	This task includes: • Validate out of the box dashboards • Review dashboards with customer • Review customer requirements in addition to standard dashboards • Disable unneeded dashboards/reports as necessary		SKILLI-PS-General (Remote)
4.5	Enable and Basic Tuning of Out of the Box Use Cases	This task includes: • A review of Out of the Box (OOTB) use cases consistent with nine (9) essential data sources on boarded during Splunk Enterprise configuration • Correlation Searches and Reports • Activity from expired user identity correlation search & proactive alert • Brute force access detected correlation search & proactive alert • Brute Force Access Detected over One Day correlation search & proactive alert • Expected Host Not Reporting correlation search & proactive alert • High Number of Hosts Not Updating Malware Signatures correlation search & alert • High Number of Infected Hosts correlation search & proactive alert • High/Critical Priority Host w/Malware Detected correlation search & proactive alert • High/Critical Priority Individual Logging into Infected Machine correlation search & proactive alert • High Volume Traffic from High/Critical Host Observed correlation search & proactive alert • Host Sending Excessive Email correlation search & proactive alert • Host with Recurring Malware Infection correlation search & proactive alert • Host with Multiple Infections correlation search & proactive alert • Host with Old Infection OR Potential Re-Infection correlation search & proactive alert • Outbreak Detected correlation search & proactive alert • Potential Gap in Data correlation search & proactive alert • Threat Activity Detected correlation search & proactive alert • Vulnerability Scanner Detected (by events) correlation search & proactive alert • Vulnerability Scanner Detected (by targets) correlation search & proactive alert		SKILLI-PS-General
Part 5: Enterprise Security - Custom Use Cases and Tuning		Consultant: Enterprise Security Specialist		
5.1	Enterprise Security Tuning	This task includes: • Core tuning of the Enterprise Security app • Configuration of Assets and Identities		SKILLI-PS-SecurityEnabled
5.2	Advanced Tuning of Out of the Box Use Cases	As necessary, given time available. This task includes: • Tuning correlation rules, searches, and proactive alerts to reduce false positives		SKILLI-PS-SecurityEnabled
5.3	Configuration of custom dashboards	As necessary, given time available. This task includes: • Configuration and deployment of up to four (4) custom views with up to four (4) searches per view • Configure and deploy custom view 1, with up to four (4) searches per view • Configure and deploy custom view 2, with up to four (4) searches per view • Configure and deploy custom view 3, with up to four (4) searches per view • Configure and deploy custom view 4, with up to four (4) searches per view		SKILLI-PS-SecurityEnabled
5.4	Review and complete installation of Enterprise Security	This task includes: • Conducting a walkthrough of ES • Notable Event Alerts • Validate notable events are populating • Demonstrate notable event workflow to customer	1	SKILLI-PS-General

Part 6: Project Close		Consultant: Enterprise Security Specialist		
6.1	Project Closeout	Activities for this task include • Production of an artifact that includes additional use cases discovered throughout the deployment • Recommendations for scaling Splunk • Review of completed SOW tasks with customer • Transition of customer to Splunk Support		SKILLI-PS-SecurityEnabled
Ongoing		Consultant: Any, as Applicable		
-	Weekly Status Reports	Splunk will provide weekly status reports	-	SKILLI-PS-General
Total			**10/13/15w**	edit as necessary

[1] http://docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware#Dedicated_search_head

[2] http://docs.splunk.com/Documentation/ES/latest/Install/DeploymentPlanning#Search_Head_considerations

[3] http://docs.splunk.com/Documentation/ES/latest/Install/DeploymentPlanning#Indexer_considerations

[4] http://docs.splunk.com/Documentation/CIM/latest/User/Overview

Assumptions
The above estimates of time for each task are based on certain assumptions:

- Durations are estimated, and work will be performed and delivered on a Time and Materials basis.
- Reasonable network and system access to configure servers, install forwarders, configure source devices, read logs, access data and applications, and allow necessary inter-system communication is all made available to Splunk resources in a timely fashion.
- Customer resources with appropriate knowledge of requirements and resources are available during the requirements phase.
- Customer resources with functional and domain knowledge are available for feedback and consultation during implementation of reporting and searching.